

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

Tatsuzo Osawa

Application. No.: to be assigned

Group Art Unit: to be assigned

Filed: January 29, 2004

Examiner: to be assigned

Title: METHOD AND APPARATUS FOR TESTING NETWORK SYSTEM, AND
COMPUTER-READABLE MEDIUM ENCODED WITH PROGRAM FOR TESTING
NETWORK SYSTEM

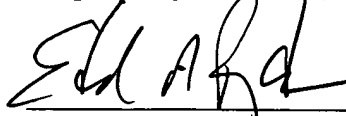
CLAIM FOR PRIORITY

Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450

Sir:

A certified copy of corresponding Japanese Application No. 2003-097431, filed March 31, 2003 is attached. It is requested that the right of priority provided by 35 U.S.C. 119 be extended by the U.S. Patent and Trademark Office.

Respectfully submitted,



Date: January 29, 2004

Edward A. Pennington, Reg. No. 32,588
Swidler Berlin Shereff Friedman, LLP
3000 K Street, NW, Suite 300
Washington, DC 20007-5116
Telephone: (202) 424-7500
Facsimile: (202) 295-8478

日 本 国 特 許 庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 3 月 3 1 日
Date of Application:

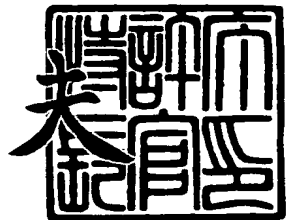
出 願 番 号 特 願 2 0 0 3 - 0 9 7 4 3 1
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 0 9 7 4 3 1]

出 願 人 富 士 通 株 式 会 社
Applicant(s):

2 0 0 4 年 1 月 7 日

特許庁長官
Commissioner,
Japan Patent Office

今 井 康



出証番号 出証特 2 0 0 3 - 3 1 0 9 1 5 9

【書類名】 特許願

【整理番号】 0253089

【提出日】 平成15年 3月31日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 13/00
G06F 15/00

【発明の名称】 ネットワークシステムテスト方法、ネットワークシステムテストプログラム及びネットワーク装置

【請求項の数】 5

【発明者】

【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

【氏名】 大澤 達蔵

【特許出願人】

【識別番号】 000005223

【氏名又は名称】 富士通株式会社

【代理人】

【識別番号】 100108187

【弁理士】

【氏名又は名称】 横山 淳一

【電話番号】 044-754-3035

【手数料の表示】

【予納台帳番号】 011280

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 0017694



【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 ネットワークシステムテスト方法、ネットワークシステムテストプログラム及びネットワーク装置

【特許請求の範囲】

【請求項 1】 ネットワーク装置の内部のデータ制御部が、ネットワークを介して接続される外部機器と該ネットワーク装置の内部に構成される複数の仮想マシンとの間で送受信される通信データを制御することにより、ネットワークシステムをテストする方法であって、

前記通信データを受信する受信ステップと、

前記通信データの属性に関する条件と、前記通信データの通信を許可するか又は廃棄するかの処理内容であるアクションとが対応付けられて設定されているテスト A C L を参照して、前記受信した通信データが、前記条件に一致するか否かを判断する判断ステップと、

前記判断ステップにおいて一致すると判断した場合には、前記通信データに対してアクションの処理内容を実施する実行ステップと

を備えたことを特徴とするネットワークシステムテスト方法。

【請求項 2】 前記通信データの属性に関する条件には、前記通信データの送信元又は受信先の、前記外部機器又は前記ネットワーク装置のネットワーク上の所在を識別するアドレス情報を含み、

前記判断ステップには、前記受信した通信データに含まれる前記アドレス情報が、前記通信データの属性に関する条件と一致するか否かの判断を含むこと

を特徴とする請求項 1 記載のネットワークシステムテスト方法。

【請求項 3】 前記受信した通信データに対して、前記判断ステップにおける条件に一致するか否かの判断に必要な属性を付加するステップを

さらに含むことを特徴とする請求項 1 記載のネットワークシステムテスト方法。

【請求項 4】 コンピュータを、ネットワークを介して接続される外部機器間で送受信される通信データを制御するネットワーク装置として動作させるためのプログラムであって、コンピュータに

前記外部機器から送信された通信データ若しくは前記ネットワーク装置の内部に構成される仮想マシンから送信された通信データを受信する受信手段と、

前記通信データの属性に関する条件と、前記通信データの通信を許可するか又は廃棄するかの処理内容であるアクションとが対応付けられて設定されているテスト A C L を参照して、前記受信した通信データが、前記条件に一致するか否かを判断する判断手段と

前記判断手段において一致すると判断した場合には、前記通信データに対してアクションの処理内容を実施する実行手段と

を機能させるためのネットワークシステムテストプログラム。

【請求項 5】 ネットワークを介して接続される外部機器間で送受信される通信データを制御するネットワーク装置において、

前記外部機器から送信された通信データ若しくは前記ネットワーク装置の内部に構成される仮想マシンから送信された通信データを受信する受信手段と、

前記通信データに関する 1 又は複数の属性に関する条件と、前記通信データが前記条件に一致した場合に前記通信データの通信を許可するか又は廃棄するかの実施すべきアクションとが対応付けられて設定されているテーブルであるテスト A C L と、

前記テスト A C L を参照して、前記受信した通信データが、前記条件に一致するか否かを判断する判断手段と、

前記判断手段において一致すると判断した場合には、前記通信データに対してアクションの処理内容を実施する実行手段と

を備えたことを特徴とするネットワーク装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、ネットワークシステムのネットワーク装置について設定等の変更を行った際の、ネットワークシステム全体の動作をテストするための方法、プログラム、装置に関する。

【0002】

【従来の技術】

従来、ネットワークシステムにおける、ファイアウォール装置、ルータ装置等のいわゆるネットワーク装置について、設定の変更やバージョンアップを行う場合には、その作業を行うために基本的にはその装置を停止させ、すなわちネットワークシステムの稼動を停止させる必要があった。このようなネットワークシステムの停止を回避するために、一部のネットワーク装置については、装置内部にハード的に複数のCPU等を備える構成としたり、ソフト的に複数の仮想マシンを装置内部に構成することにより、ネットワーク装置内部に複数のネットワーク装置の機能を構成して、設定の変更後のシステムをあらかじめ保持し、瞬時に稼動するシステムを切り替えることで、ネットワークシステムの停止時間を最小化するものも存在する。

【0003】

また、特許文献1には、ファイアウォール装置の内部に複数の仮想マシンを構成することが記載されている。

【0004】**【特許文献1】**

特開2001-318797号公報

【0005】**【発明が解決しようとする課題】**

しかし、従来の技術によれば、変更作業そのものによる停止時間は最小化することはできても、ネットワークシステムはネットワーク装置と、接続される外部機器とが密結合して構成するシステムであることから、設定変更のミスやネットワーク装置を制御する新バージョンのソフトウェアの不具合によって、変更後のネットワークシステムに不具合が生じることがあった。これを防止するためには、前記のような設定の変更等は、不具合が発生しても影響の少ない深夜等の閑散時間帯に行うか、本稼動の前にテストのための時間を割く必要があった。すなわち、結局は、ネットワークシステムを本稼動できない時間が発生することになってしまっていた。

そこで、本発明は、ネットワーク装置の設定等の変更の際に、ネットワークシス

テムを停止することなく、変更後の設定のミスや不具合等を排除するためのテストを行う方法を提供することを目的とするものである。

【0006】

【課題を解決するための手段】

本発明のネットワークシステムテスト方法は、ネットワークを介して接続される外部機器と該ネットワーク装置の内部の仮想マシンとの間で送受信される通信データを受信する受信ステップと、前記通信データの属性に関する条件と、前記通信データの通信を許可するか又は廃棄するかの処理内容であるアクションとが対応付けられて設定されているテストACL (Access Control List) を参照して、前記受信した通信データが、前記条件に一致するか否かを判断する判断ステップと、一致すると判断した場合には、前記通信データに対してアクションの処理内容を実施する実行ステップとを含むものである。

【0007】

従って、本発明によれば、ネットワークシステムを停止させることなく、変更後の設定によるシステムのテストを行うことが可能となる。

【0008】

【発明の実施の形態】

本発明の実施の形態について図面により説明する。

【0009】

図1に本発明の実施例の接続構成を示す。サーバ25と運用クライアント21、23がネットワーク26を介して接続されているシステムであるが、サーバ25とクライアント装置はネットワーク装置10を経由して接続される。このネットワーク装置10は、ファイアウォール装置、ルータ装置等のような、ネットワーク上で送受信される通信データを適切に制御するための装置である。ここで、通常の運用は、運用クライアント21、23により行われているが、ネットワーク装置10の変更後の設定をテストするための専用のクライアント装置として、テストクライアント22、24が接続されている。各装置に括弧書きで示したのは、ネットワーク26上における識別情報であるIPアドレスである。

【0010】

図 2 にネットワーク装置 1 0 の内部構成の概要を示す。データ制御部 1 1 は外部機器群 2 0 とネットワーク装置 1 0 の内部に構成される運用系仮想マシン 1 5 やテスト系仮想マシン 1 6 との間で送受信される通信データを制御する機能を備えるものである。この外部機器群 2 0 は前記のサーバ 2 5、テストクライアント 2 2、2 4、運用クライアント 2 1、2 3 等を総称したものである。データ制御部 1 1 には、テスト A C L 1 2、内向け通信判定プログラム 1 3、外向け通信判定プログラム 1 4 を備えている。内向け通信判定プログラム 1 3 は、外部機器群 2 0 から受信した通信データについて、テスト A C L 1 2 を参照して属性の条件が一致するか否かを判断し、一致した場合には該当するアクションの内容を実施するための処理を記述したプログラムである。外向け通信判定プログラム 1 4 は、仮想マシンから受信した通信データについて、テスト A C L 1 2 を参照して属性の条件が一致するか否かを判断し、一致した場合には該当するアクションの内容を実施するための処理を記述したプログラムである。運用系仮想マシン 1 5 は、稼動中のネットワーク装置 1 0 としての機能を実現しているものである。テスト系仮想マシン 1 6 は、基本的な構成としては運用系仮想マシン 1 5 と同等でありネットワーク装置としての機能を発揮するものであるが、変更後の設定を施してある点で相違する。それぞれの仮想マシンは、それぞれに仮想 C P U 1 7、仮想メモリ 1 8 を備えており、あたかも 1 つの独立した装置として動作するように構成されている。この仮想マシンはハードとしては 1 個の C P U により動作するネットワーク装置内に、ソフト的に複数のマシンとして動作するよう構成される場合もあるし、あるいは、1 台のネットワーク装置内に複数の C P U を備え、ハード的に独立した C P U を備えるものとして構成される場合もある。

【 0 0 1 1 】

テスト A C L 1 2 は、通信データの属性に関する 1 又は複数の条件と、通信を許可するか又は廃棄するかアクションとが対応付けられて設定されているテーブルであり、データ制御部 1 1 が、受信した通信データの属性に関する条件が一致するか否かを判定し、一致していた場合には、アクションに設定されている処理内容を実施する。本実施例のテスト A C L 1 2 は図 3 に示すように識別子 3 1、処理を実施すべき仮想マシン 3 2、通信識別条件 3 3 が、通信データの属性に

関する条件として設定されており、それらが一致した場合にアクション 34 に設定されている廃棄か許可の処理を行うのである。廃棄の処理は、文字通り通信データをその時点で廃棄し、データ制御部の外部には出力しないことである。許可の処理は、内向けであれば属性で指定された仮想マシンに対して通信データを送信し、外向けであれば、通信データを外部に対して出力する。

【0012】

図4は、設定の変更のテストを行うために、実際に稼動しているものとは別にネットワーク 26 に接続したテストクライアントの IP アドレスを設定したテストクライアント IP アドレスリスト 40 である。本実施例では、テスト ACL 12 の通信識別条件として、通信データの送信元か受信先がテストクライアントであることを判定の条件として設定していることから、テストクライアントの IP アドレスの情報が必要であるため、このテストクライアント IP アドレスリストが必要になる。なお、このテストクライアント IP アドレスリスト 40 は、図2では図示はしていないが、データ制御部 11 に備えるものである。

【0013】

図5は、データ制御部 11 において、テスト ACL 12 を参照して判定する処理の前に、通信データに対して必要に応じて属性を付加した場合の例を示している。詳細は後述する。

【0014】

次に、図6乃至図8に示すフローチャートを用いて、本発明の動作例を説明する。通常の通信データの送受信において、ある外部機器から他の外部機器に送信される場合は、まず送信元の外部機器から通信データが送信されネットワーク装置 10 で受信される。ここまでの前半部分の処理は図6で説明する。そして、ネットワーク装置 10 で適当な処理が行われた後に、ネットワーク装置 10 から通信データが送信され、受信先の外部機器により受信される。この後半部分の処理は図7で説明する。

【0015】

図6は、データ制御部 11 が、サーバ、クライアント等の外部機器群 20 から通信データを受信したときに、テスト ACL 12 を参照して、通信データに対す

るアクションを判定する処理を説明するためのフローチャートである。

【0016】

まずステップS61では、外部機器群20より通信データ51を受信する。ここで受信する通信データ51は図5(a)に示すとおり、少なくとも送信元IPアドレスを受信先IPアドレスとデータとを含むものである。この通信データ51が、テストクライアント22からサーバ25に対して送信されたものならば、送信元IPアドレスにはテストクライアント22のIPアドレスが設定されており、受信先IPアドレスにはサーバ25のIPアドレスが設定されている。

【0017】

ステップS62では、テストACL12が有効か否かを判断する。すなわち、テストACL12が有効であるということは、ネットワーク装置10の変更後の設定のテストを行おうとしている状態であり、有効でないということは、特に新たな設定をテストしようとしているわけではなく、通常の稼動をしている状態である。なお図示はしていないが、この判断は、例えば、いずれかのメモリにテストACL12が有効か否かを示すフラグ領域を設けて、それを参照することにより判断するものとしてもよい。ステップS62で有効でないと判断した場合には、ステップS64に進む。

【0018】

ステップS64では、受信した通信データ51を運用系仮想マシン15に送信する。ネットワーク装置の変更後の設定のテストを行おうとしている状態ではないため、外部機器群20から受信した通信データ51はすべて通常稼動状態のものであるので、ネットワーク装置10による通信データ51の処理は運用系仮想マシン15で行われる。

【0019】

ステップS63では受信した通信データ51を図5の(b)、(c)のように、運用系仮想マシン用通信データ52とテスト系仮想マシン用通信データ53とにコピーする。その際に、外部機器群20からネットワーク装置10内部の仮想マシン向けの通信データであることを示す「内向け」のフラグと、運用系仮想マシン15向けの通信データ52であることを示す「運用系」フラグと、テスト系

仮想マシン 16 向けの通信データ 53であることを示す「テスト系」フラグとを付加する。後に適切に許可又は削除の判断がされることを前提として、ここでは一時的にそれぞれの仮想マシン向けの通信データを生成するのである。

【0020】

ステップ S65では、テスト ACL 12の1ライン目の属性に関する条件を参照する。

【0021】

そして、ステップ S66で、運用系仮想マシン用通信データ 52とテスト系仮想マシン用通信データ 53とのそれぞれに対して、テスト ACL 12の属性に関する条件と一致するか否かを判断する。

【0022】

この判断の処理の詳細を図8に示す。先ずステップ S81では識別子 31を参照して、通信データの「内向け」又は「外向け」フラグと一致するか否かを判断する。ここで「内向け」とは、外部機器群 20からネットワーク装置 10内の仮想マシンに送信される通信データであることを示す。また「外向け」とは、逆に、仮想マシンから外部機器群 20に送信される通信データであることを示す。次にステップ S82では、通信データに設定された仮想マシンの種類を示すフラグと、仮想マシン 32のフィールドを参照して、一致するか否かを判断する。そして、ステップ S83では、通信データの送信元の IP アドレス又は受信先の IP アドレスが、通信識別条件 33に設定した条件と一致するか否かを判断する。例えば、テスト ACL 12の1ライン目であれば、送信元又は受信先がテストクライアントであるか否かを IP アドレスを用いて判断する。その際には図4に示すテストクライアント IP アドレスリスト 40を参照する。

【0023】

上記のステップ S81、ステップ S82、ステップ S83ですべて一致すると判断すれば、ステップ S66についてテスト ACL 12のそのラインの属性に関する条件に一致すると判断し、1ステップでも一致しなければ、不一致と判断する。

【0024】

ステップ S 6 6 で不一致と判断するとステップ S 6 7 に進み、テスト A C L 1 2 の次のラインを参照して再びステップ S 6 6 に進み、条件に一致するか否かを判断する。ステップ S 6 6 で一致と判断すれば、ステップ S 6 8 に進み、アクション 3 4 に設定されている廃棄か許可の処理を実行する。「廃棄」とは、文字通りその通信データをデータ制御部 1 1 から何に対しても出力しないことを意味する。「許可」とは、内向きの通信データであれば、運用系かテスト系の仮想マシンに対して出力することを意味し、外向きであれば、ネットワーク装置 1 0 から外部機器群 2 0 に対して出力することを意味する。

【 0 0 2 5 】

図 7 は、データ制御部 1 1 が、運用系仮想マシン 1 5 又はテスト系仮想マシン 1 6 から通信データを受信したときに、テスト A C L 1 2 を参照して、通信データに対するアクションを判定する処理を説明するためのフローチャートである。

【 0 0 2 6 】

まずステップ S 7 0 1 では、仮想マシンより通信データを受信する。

【 0 0 2 7 】

ステップ S 7 0 2 では、テスト A C L 1 2 が有効か否かを判断する。すなわち、テスト A C L 1 2 が有効であるということは、ネットワーク装置 1 0 の変更後の設定のテストを行おうとしている状態であり、有効でないということは、特に新たな設定をテストしようとしているわけではなく、通常の稼動をしている状態である。ステップ S 7 0 2 で有効でないと判断した場合には、ステップ S 7 0 3 に進む。

【 0 0 2 8 】

ステップ S 7 0 3 では、受信した通信データがテスト系仮想マシン 1 6 からのものか否かを判断する。テスト系仮想マシン 1 6 からのものと判断すれば、その状態では設定のテストを行おうとしている状態ではないので、その通信データは廃棄し、そうでなければ、通常の稼動による通信データであるので、そのまま外部機器群 2 0 に対して送信する。

【 0 0 2 9 】

ステップ S 7 0 6 では受信した通信データに対して、テスト A C L 1 2 を用い

た判断を行うために、適当なフラグを付加する。受信した通信データが運用系仮想マシン 15 からのものであれば、図 5 の (d)、(e) のように「運用系」フラグと「外向け」フラグを付加する。受信した通信データが、テスト系仮想マシン 16 からのものであれば、図 5 の (f)、(g) のように「テスト系」フラグと「外向け」フラグを付加する。

【0030】

以降のステップ S 707 乃至ステップ S 710 の処理は、図 6 のステップ S 65 乃至ステップ S 68 の処理と同様である。

【0031】

次に、図 9 乃至図 10 により本発明の具体的な処理の例を説明する。

【0032】

図 9 はサーバ 25 から運用クライアント 21 に対するデータの送信の例であり、この送信は、テストではなく通常の運用によるものである。

【0033】

サーバ 25 から送信される通信データ 91 には、送信元であるサーバ 25 の IP アドレス「111.222.333.100」と受信先の運用クライアント 21 の IP アドレス「111.222.333.001」が設定されており、この通信データ 91 がデータ制御部 11 に送信されると、運用系仮想マシン向け通信データ 92 とテスト系仮想マシン向け通信データ 93 にコピーされ、それぞれのデータをあらわす「運用」フラグと「テスト」フラグが付与され、さらに外部機器群 20 から仮想マシン向けのデータであることを示す「内向け」フラグが付与される。

【0034】

データ制御部 11 では、図 6 のステップ S 65 乃至ステップ S 67、及び図 8 のフローチャートに従って、運用系仮想マシン向け通信データ 92 とテスト系仮想マシン向け通信データ 93 とのそれぞれについて、テスト ACL 12 に設定された条件についてライン No. 1 から順に比較する。図 9 中で (a) で表される運用系仮想マシン向け通信データ 92 は、送信元も受信先もテストクライアントではなく、受信先がネットワーク装置 10 でもないため、ライン No. 1～ライ

ンNo. 5とは一致せず、運用系仮想マシン向けであることを示す「運用」フラグを有することから、ラインNo. 6にも一致せずに、ラインNo. 7と一致する。したがって、運用系仮想マシン向け通信データ92は、ラインNo. 7のアクション34に設定されているとおり、通信を「許可」され通信データは運用系仮想マシン15に送信される。また、図9中で(b)で表されるテスト系仮想マシン向け通信データ93は、送信元も受信先もテストクライアントではなく、受信先がネットワーク装置10でもないため、ラインNo. 1～ラインNo. 5とは一致せず、テスト系仮想マシン向けであることを示す「テスト」フラグを有することから、ラインNo. 6に一致する。したがって、テスト系仮想マシン向け通信データ93は、ラインNo. 6のアクション34に設定されているとおり、「廃棄」される。

【0035】

運用系仮想マシン15に送信された通信データ94は、ネットワーク装置10としての機能による処理を運用系仮想マシン15でされた後、データ制御部11に送信される。データ制御部11は、送信された通信データ94に、運用系仮想マシン15からの通信データであることを示す「運用」フラグと、仮想マシンから外部機器群20に対する通信データであることを示す「外向け」フラグを付与し、テストACL12と比較する外向けデータ95とする。この外向けデータ95は、送信元も受信先もテストクライアントではなく、受信先がネットワーク装置10でもないため、ラインNo. 1～ラインNo. 5とは一致せず、運用系仮想マシン向けであることを示す「運用」フラグを有することから、ラインNo. 6にも一致せずに、ラインNo. 7と一致する。したがって、外向け通信データ95は、ラインNo. 7のアクション34に設定されているとおり、通信を「許可」され通信データは運用クライアント21に送信される。

【0036】

以上のように、サーバ25から運用クライアント21に送信される通信データは、ネットワーク装置10においては、運用系仮想マシン15によって適切に処理され、通常の稼動状態と全く変わらずに、通信を行うことができる。

【0037】

図10はテストクライアント22からサーバ25に対するデータの送信の例であり、この送信は、テストクライアントによって、ネットワーク装置10のテストを行うための通信である。

【0038】

テストクライアント22から送信される通信データ101には、送信元であるテストクライアント22のIPアドレス「111.222.333.002」と受信先のサーバ25のIPアドレス「111.222.333.100」が設定されており、この通信データ101がデータ制御部11に送信されると、運用系仮想マシン向け通信データ102とテスト系仮想マシン向け通信データ103にコピーされ、それぞれのデータをあらわす「運用」フラグと「テスト」フラグが付与され、さらに外部機器群20から仮想マシン向けのデータであることを示す「内向け」フラグが付与される。

【0039】

データ制御部11では、図7のステップS707乃至ステップS710、及び図8のフローチャートに従って、運用系仮想マシン向け通信データ102とテスト系仮想マシン向け通信データ103とのそれぞれについて、テストACL12に設定された条件についてラインNo. 1から順に比較する。図10中で(a)で表される運用系仮想マシン向け通信データ102は、送信元がテストクライアントであり、運用系仮想マシン向けであることを示す「運用」フラグと「内向け」フラグを有することから、ラインNo. 1と一致する。したがって、運用系仮想マシン向け通信データ102は、ラインNo. 1のアクション34に設定されているとおり、「廃棄」される。また、図10中で(b)で表されるテスト系仮想マシン向け通信データ103は、送信元がテストクライアントであり、テスト系仮想マシン向けであることを示す「テスト」フラグと「内向け」フラグを有することから、ラインNo. 2に一致する。したがって、テスト系仮想マシン向け通信データ103は、ラインNo. 2のアクション34に設定されているとおり、通信を「許可」されはテスト系仮想マシン16に送信される。

【0040】

テスト系仮想マシン16に送信された通信データ104は、変更後の設定にか

かるネットワーク装置 10 としての機能による処理をテスト系仮想マシン 16 で行われた後、データ制御部 11 に送信される。データ制御部 11 は、送信された通信データ 104 に、テスト系仮想マシン 16 からの通信データであることを示す「テスト」フラグと、仮想マシンから外部機器群 20 に対する通信データであることを示す「外向け」フラグを付与し、テスト ACL 12 と比較する外向けデータ 105 とする。この外向けデータ 105 は、送信元がテストクライアントであり、テスト系仮想マシン向けであることを示す「テスト」フラグを有することから、ライン No. 1 ~ No. 3 には一致せずに、ライン No. 4 と一致する。したがって、外向け通信データ 105 は、ライン No. 4 のアクション 34 に設定されているとおり、通信を「許可」され通信データはサーバ 25 に送信される。

【0041】

以上のように、テストクライアント 22 からサーバ 25 に送信される通信データは、ネットワーク装置 10 においては、変更後の設定が施されたテスト系仮想マシン 16 によって適切に処理され、通常の稼動を妨げることなく、変更後の設定を確認するための通信を行うことができる。

【0042】

以上に述べた本発明の実施例、動作例においては、テスト ACL 12 は、外部機器から送信される「内向き」の通信データに関する条件と、仮想マシンから送信される「外向き」の通信データに関する条件とを 1 つのテーブルに設定し、すべての通信データについてその 1 つのテスト ACL 12 を参照することとしたが、本発明はそのような構成に限られるものではない。

【0043】

図 11 は、外部機器から仮想マシン向けの通信データと、仮想マシンから外部機器向けの通信データとを別に扱い、それぞれに対するテスト ACL を別に備えた場合の例である。図 12 に示す外部機器から仮想マシン向けの打ち向けの通信データ 121 は、データ制御部 11 において、「運用系」フラグを付加された運用系仮想マシン向け通信データ 122 と、「テスト系」フラグを付加されたテスト系仮想マシン向け通信データ 123 とにコピーされ、それぞれ外部機器から仮

想マシン向けのテストACL110と比較を行う。そこで条件が一致すればアクションに設定された廃棄か許可の処理を行い、一致しなければ両方向の通信データのテストACL112を参照して、そこで条件が一致したラインNo. のアクションに設定された処理を行う。運用系仮想マシンから外部機器向けの通信データ124は、データ制御部11において、「運用系」フラグを付加され外部機器向け通信データ125とし、仮想マシンから外部機器向けの通信データのテストACL111の各ラインNo. の条件と比較をし、条件が一致すればアクションに設定された処理を行う。一致しなければ両方向の通信データのテストACL112を参照して、そこで条件が一致したラインNo. のアクションに設定された処理を行う。テスト系仮想マシンから外部機器向けの通信データ126は、データ制御部11において、「テスト系」フラグを付加され外部機器向け通信データ127とし、仮想マシンから外部機器向けの通信データのテストACL111の各ラインNo. の条件と比較をし、条件が一致すればアクションに設定された処理を行う。一致しなければ両方向の通信データのテストACL112を参照して、そこで条件が一致したラインNo. のアクションに設定された処理を行う。

【0044】

ここまでは通信識別条件としてクライアントのIPアドレスを設定する場合について実施例として示したが、それ以外の条件を通信識別条件に設定することも可能である。その場合の第2の実施例を図13乃至図15を用いて説明する。

【0045】

図13は本実施例の構成を示したものであり、クライアント131とサーバ132とがネットワーク26及びネットワーク装置10を介して接続されている。サーバ132には、実稼動中の既存アプリケーション134と、これから新規に追加し稼動テストを行おうとしている新規アプリケーション133が存在している。本実施例は、既存アプリケーション134の稼動状態に影響を与えずに、新規アプリケーション133を疎通させるためのネットワーク装置10の動作、及びネットワークのシステム全体の動作のテストを行うことを目的とする。図14に示す本実施例におけるテストACLは、図11に示すテストACLと類似の構成となっているが、通信識別条件に設定される項目が異なっている。テストAC

Lの各ラインNo. に設定する条件として、ある通信データが新規アプリケーション133に対するものであるか否かにより、判定を行うものとしている。新規アプリケーションに対する通信データを識別する方法としてはいくつか考えられる。例えば図13に示すような同一のサーバ132に既存アプリケーション134と新規アプリケーションを併存させるのではなく、別のサーバにそれぞれ搭載させることとするならば、通信識別条件としては、新規アプリケーション133を搭載したサーバのIPアドレスにより判定するものとすればよい。また、図13のような構成とした場合であって、サーバ132のTCP (Transmission Control Protocol) サービスポートにより区別されている場合には、テストACL140、141、142の通信識別条件として、TCPサービスポートを設定しておき、通信データに含まれるTCPサービスポートにより判定するものとすればよい。

【0046】

図示はしていないが、ネットワーク装置10は、CPU (Central Processing Unit) によって装置全体が制御されているコンピュータの1種である。CPUには、バスを介してRAM (Random Access Memory)、ハードディスク装置 (HDD)、入出力インタフェース、および通信インタフェース等が接続されている。

【0047】

RAMには、CPUに実行させるOS (Operating System) のプログラムやその他のプログラムの少なくとも一部が一時的に格納される。また、RAMには、CPUによる処理に必要な各種データが格納される。HDDには、OSやその他のプログラムおよびデータが格納される。

【0048】

本発明の実施の形態に係る図6乃至図8に示すフローチャートで説明した処理は、プログラム及びソフトウェアとして提供されるものであり、それらのプログラムをコンピュータで実行させることによって、コンピュータをネットワーク装置10として機能させることができる。

【0049】

また、上記のコンピュータが有すべき機能の処理内容は、コンピュータで読み取り可能な記録媒体に記録されたプログラムに記述しておくことができる。このプログラムをコンピュータで実行することにより、上記処理がコンピュータで実現できる。コンピュータで読み取り可能な記録媒体としては、磁気記録装置や半導体メモリなどがある。市場に流通させる場合には、C D - R O M (Compact Disk Read Only Memory) やフレキシブルディスクなどの可搬型記録媒体にプログラムを格納して流通させたり、ネットワークを介して接続されたコンピュータの記憶装置に格納しておき、ネットワークを通じて他のコンピュータに転送したりすることもできる。コンピュータで実行する際には、コンピュータ内のハードディスク装置などにプログラムを格納しておき、メインメモリにロードして実行する。

【 0 0 5 0 】

(付記 1)

ネットワーク装置の内部のデータ制御部が、ネットワークを介して接続される外部機器と該ネットワーク装置の内部に構成される複数の仮想マシンとの間で送受信される通信データを制御することにより、ネットワークシステムをテストする方法であって、

前記通信データを受信する受信ステップと、

前記通信データの属性に関する条件と、前記通信データの通信を許可するか又は廃棄するかの処理内容であるアクションとが対応付けられて設定されているテスト A C L を参照して、前記受信した通信データが、前記条件に一致するか否かを判断する判断ステップと、

前記判断ステップにおいて一致すると判断した場合には、前記通信データに対してアクションの処理内容を実施する実行ステップと

を備えたことを特徴とするネットワークシステムテスト方法。

【 0 0 5 1 】

(付記 2)

前記通信データの属性に関する条件には、前記通信データの送信元又は受信先の、前記外部機器又は前記ネットワーク装置のネットワーク上の所在を識別する

アドレス情報を含み、

前記判断ステップには、前記受信した通信データに含まれる前記アドレス情報が、前記通信データの属性に関する条件と一致するか否かの判断を含むことを特徴とする付記 1 記載のネットワークシステムテスト方法。

【 0 0 5 2 】

(付記 3)

前記受信した通信データに対して、前記判断ステップにおける条件に一致するか否かの判断に必要な属性を付加するステップを

さらに含むことを特徴とする付記 1 記載のネットワークシステムテスト方法。

【 0 0 5 3 】

(付記 4)

コンピュータを、ネットワークを介して接続される外部機器間で送受信される通信データを制御するネットワーク装置として動作させるためのプログラムであって、コンピュータに

前記外部機器から送信された通信データ若しくは前記ネットワーク装置の内部に構成される仮想マシンから送信された通信データを受信する受信手段と、

前記通信データの属性に関する条件と、前記通信データの通信を許可するか又は廃棄するかの処理内容であるアクションとが対応付けられて設定されているテスト A C L を参照して、前記受信した通信データが、前記条件に一致するか否かを判断する判断手段と

前記判断手段において一致すると判断した場合には、前記通信データに対してアクションの処理内容を実施する実行手段と

を機能させるためのネットワークシステムテストプログラム。

【 0 0 5 4 】

(付記 5)

前記通信データの属性に関する条件には、前記通信データの送信元又は受信先の、前記外部機器又は前記ネットワーク装置のネットワーク上の所在を識別するアドレス情報を含み、

前記判断手段では、前記受信した通信データに含まれる前記アドレス情報が、前記通信データの属性に関する条件と一致するか否かの判断を含むことを特徴とする付記 4 記載のネットワークシステムテストプログラム。

【 0 0 5 5 】

(付記 6)

前記受信した通信データに対して、前記判断手段における条件に一致するか否かの判断に必要な属性を付加する属性付加手段を

さらに含むことを特徴とする付記 4 記載のネットワークシステムテストプログラム。

【 0 0 5 6 】

(付記 7)

ネットワークを介して接続される外部機器間で送受信される通信データを制御するネットワーク装置において、

前記外部機器から送信された通信データ若しくは前記ネットワーク装置の内部に構成される仮想マシンから送信された通信データを受信する受信手段と、

前記通信データに関する 1 又は複数の属性に関する条件と、前記通信データが前記条件に一致した場合に前記通信データの通信を許可するか又は廃棄するかの実施すべきアクションとが対応付けられて設定されているテーブルであるテスト A C L と、

前記テスト A C L を参照して、前記受信した通信データが、前記条件に一致するか否かを判断する判断手段と、

前記判断手段において一致すると判断した場合には、前記通信データに対してアクションの処理内容を実施する実行手段と

を備えたことを特徴とするネットワーク装置。

【 0 0 5 7 】

(付記 8)

前記通信データの属性に関する条件には、前記通信データの送信元又は受信先の、前記外部機器又は前記ネットワーク装置のネットワーク上の所在を識別するアドレス情報を含み、

前記判断手段では、前記受信した通信データに含まれる前記アドレス情報が、前記通信データの属性に関する条件と一致するか否かの判断を含むことを特徴とする付記 7 記載のネットワークシステムテスト装置。

【 0 0 5 8 】

(付記 9)

前記受信した通信データに対して、前記判断手段における条件に一致するか否かの判断に必要な属性を付加する属性付加手段を

さらに含むことを特徴とする付記 7 記載のネットワークシステムテスト装置。

【 0 0 5 9 】

【発明の効果】

以上説明したように、本発明によれば、ネットワーク装置の設定等の変更の際に、稼動しているネットワークシステムに影響を与えたり停止させたりすることなく、変更後の設定のミスや不具合等を排除するためのテストを行うことが可能となる。

【図面の簡単な説明】

【図 1】 本発明にかかるネットワーク装置の構成図である。

【図 2】 本発明の実施の形態にかかる接続構成図である。

【図 3】 実施の形態にかかるテスト A C L の構成を図示したものである。

【図 4】 テストクライアント I P アドレスリストを図示したものである。

【図 5】 実施の形態にかかる通信データの例を図示したものである。

【図 6】 内向け通信判定プログラムの処理を説明するフローチャートである。

【図 7】 外向け通信判定プログラムの処理を説明するフローチャートである。

【図 8】 通信データをテスト A C L の条件と比較する処理を説明するフローチャートである。

【図 9】 本発明の具体的な動作例を図示したものである。

【図 1 0】 本発明の具体的な動作例を図示したものである。

【図 1 1】 実施の形態にかかるテスト A C L の構成の例を図示したものである。

【図 1 2】 実施の形態にかかる通信データの例を図示したものである。

【図 1 3】 第 2 の実施例にかかる接続構成図である。

【図 1 4】 第 2 の実施例にかかるテスト A C L の構成の例を図示したものである

。

【符号の説明】

- 1 0 ネットワーク装置
- 1 1 データ制御部
- 1 2 テスト A C L
- 1 3 内向け通信判定プログラム
- 1 4 外向け通信判定プログラム
- 1 5 運用系仮想マシン
- 1 6 テスト系仮想マシン
- 1 7 仮想メモリ
- 1 8 仮想 C P U
- 2 0 外部機器群
- 2 1 運用クライアント
- 2 2 テストクライアント
- 2 3 運用クライアント
- 2 4 テストクライアント
- 2 5 サーバ
- 2 6 ネットワーク
- 3 1 テスト A C L の識別子を設定するフィールド
- 3 2 テスト A C L の仮想マシンを設定するフィールド
- 3 3 テスト A C L の通信識別条件を設定するフィールド
- 3 4 テスト A C L のアクションを設定するフィールド
- 3 5 テスト A C L のライン N o を設定するフィールド
- 4 0 テストクライアント I P アドレスリスト
- 5 1、9 1、1 0 1、1 2 1 外部機器から送信された通信データ
- 5 2、9 2、1 0 2、1 2 2 運用系仮想マシン用通信データ
- 5 3、9 3、1 0 3、1 2 3 テスト系仮想マシン用通信データ
- 5 4、9 4、1 2 4 運用系仮想マシンから送信された通信データ

55、95、125 運用系仮想マシンから送信されフラグを付加した通信データ

56、104、126 テスト系仮想マシンから送信された通信データ

57、95、105、127 テスト系仮想マシンから送信されフラグを付加した通信データ

96、106 ネットワーク装置から外部機器に送信された通信データ

110、140 外部機器から仮想マシン向けの通信データのテストACL

111、141 仮想マシンから外部機器向けの通信データのテストACL

112、142 両方向の通信データのテストACL

131 クライアント

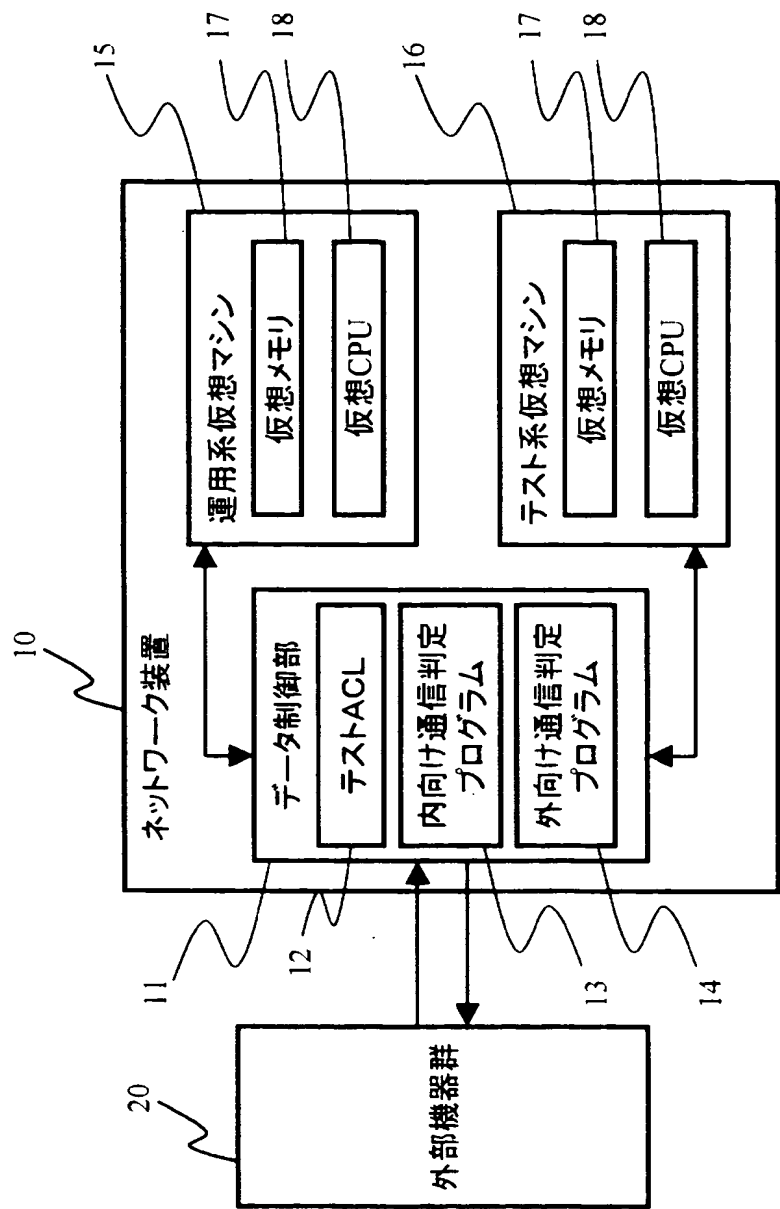
132 サーバ

133 新規アプリケーション

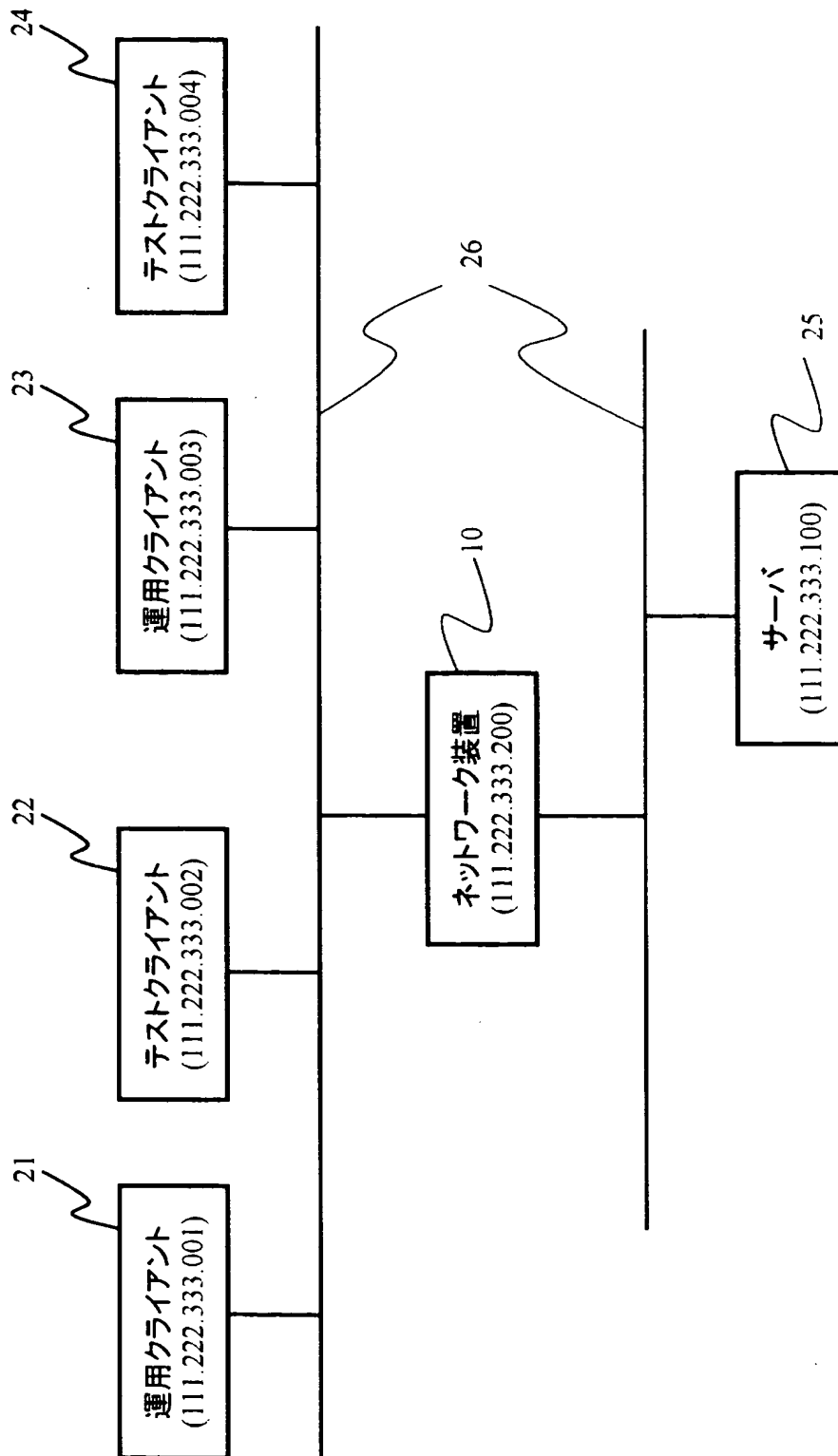
134 既存アプリケーション

【書類名】 図面

【図 1】



【図 2】



【図 3】

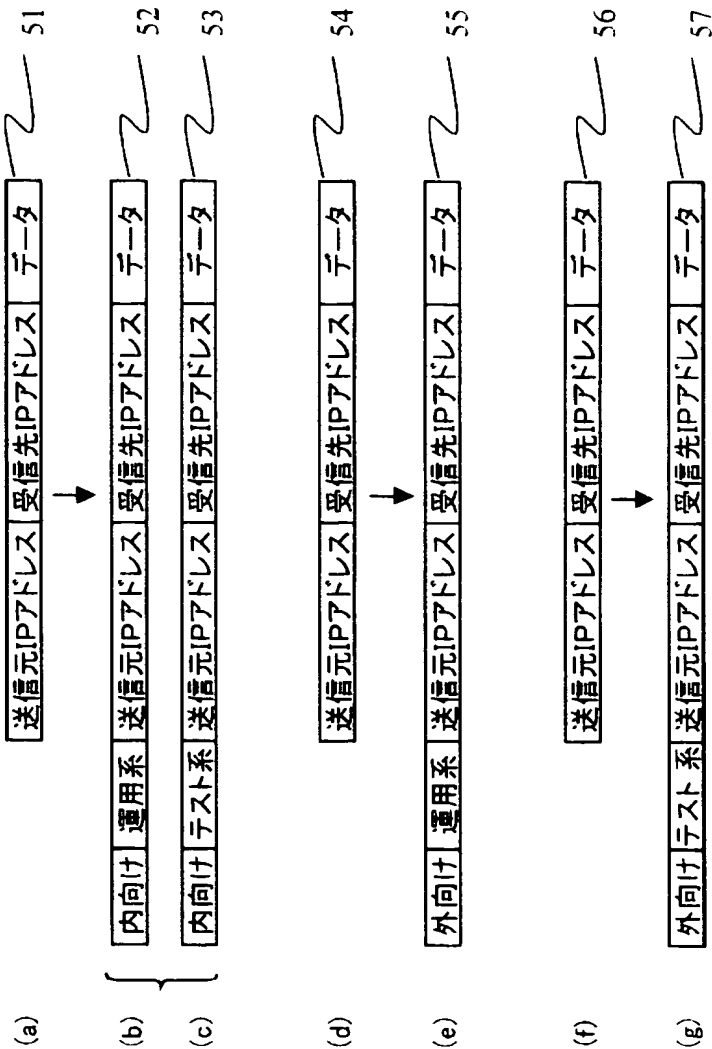
ラインNo	識別子	仮想マシン	通信識別条件	アクション
1	内向け	運用系	送信元又は受信先がテストクライアント	廃棄
2	内向け	テスト系	送信元又は受信先がテストクライアント	許可
3	外向け	運用系	送信元又は受信先がテストクライアント	廃棄
4	外向け	テスト系	送信元又は受信先がテストクライアント	許可
5	両方向	運用系又はテスト系	受信先が本ネットワーク装置	許可
6	両方向	テスト系	全て	廃棄
7	両方向	運用系	全て	許可

【図 4】

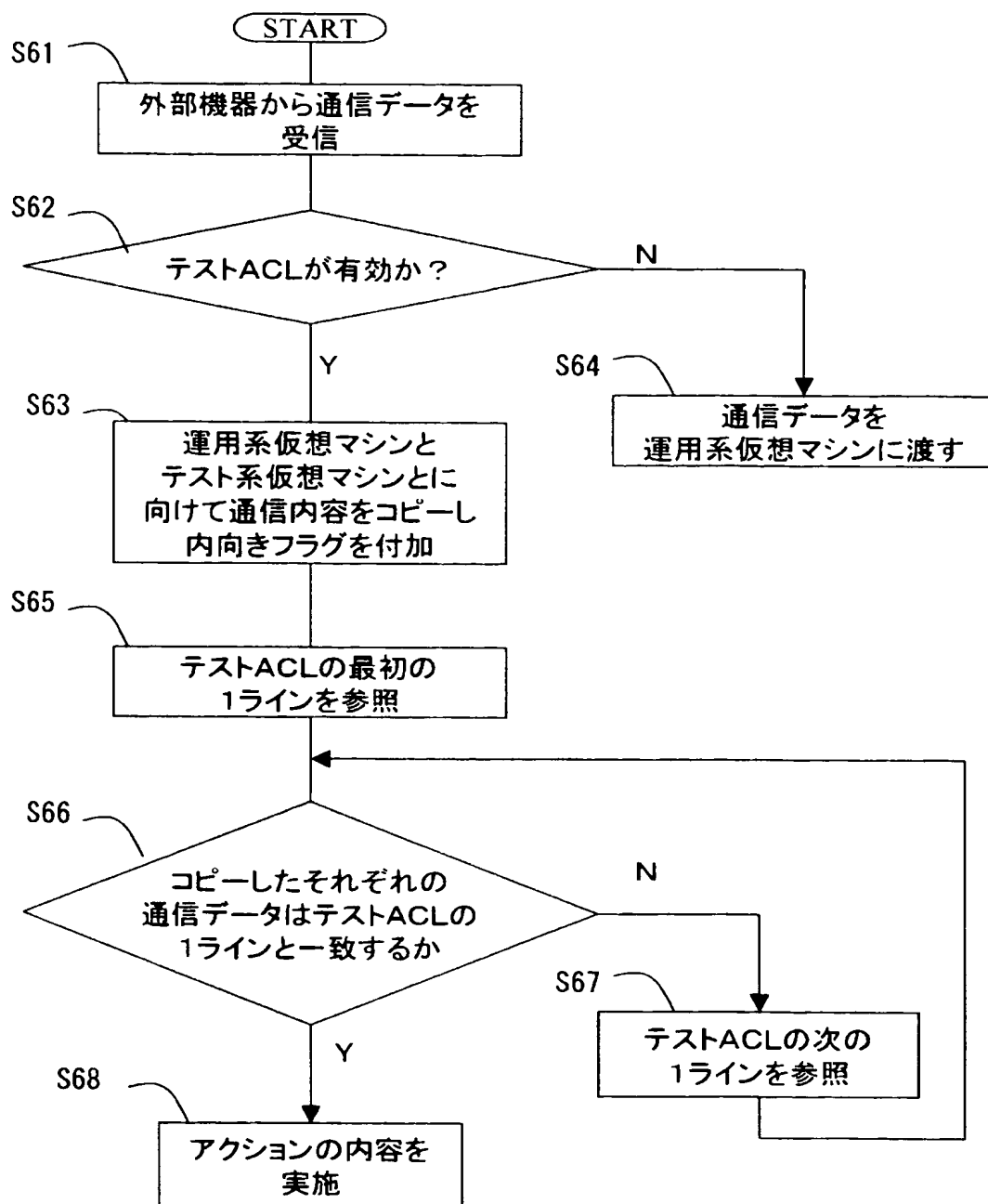
40

テストクライアントIPアドレスリスト
111.222.333.002
111.222.333.004

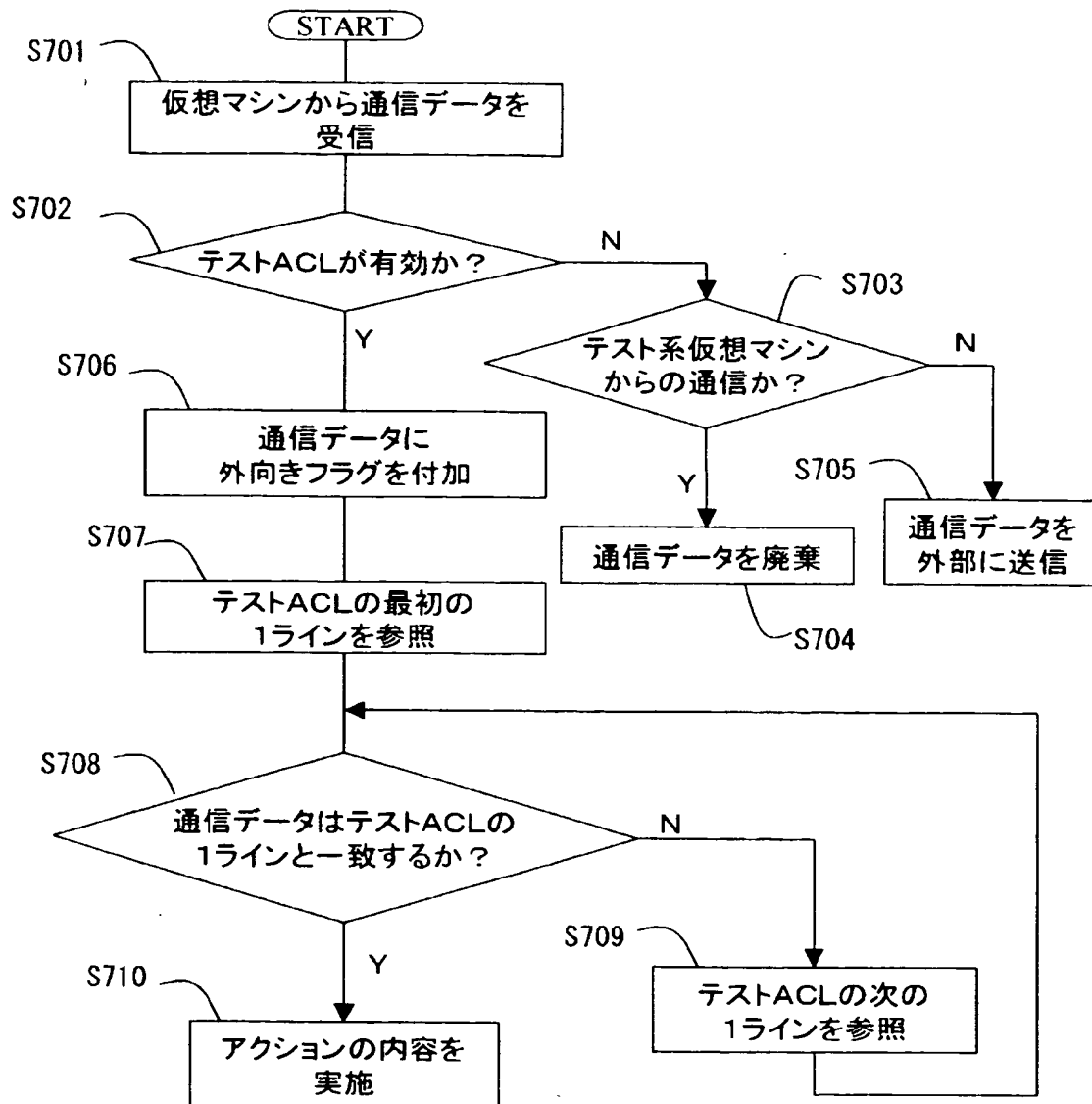
【図 5】



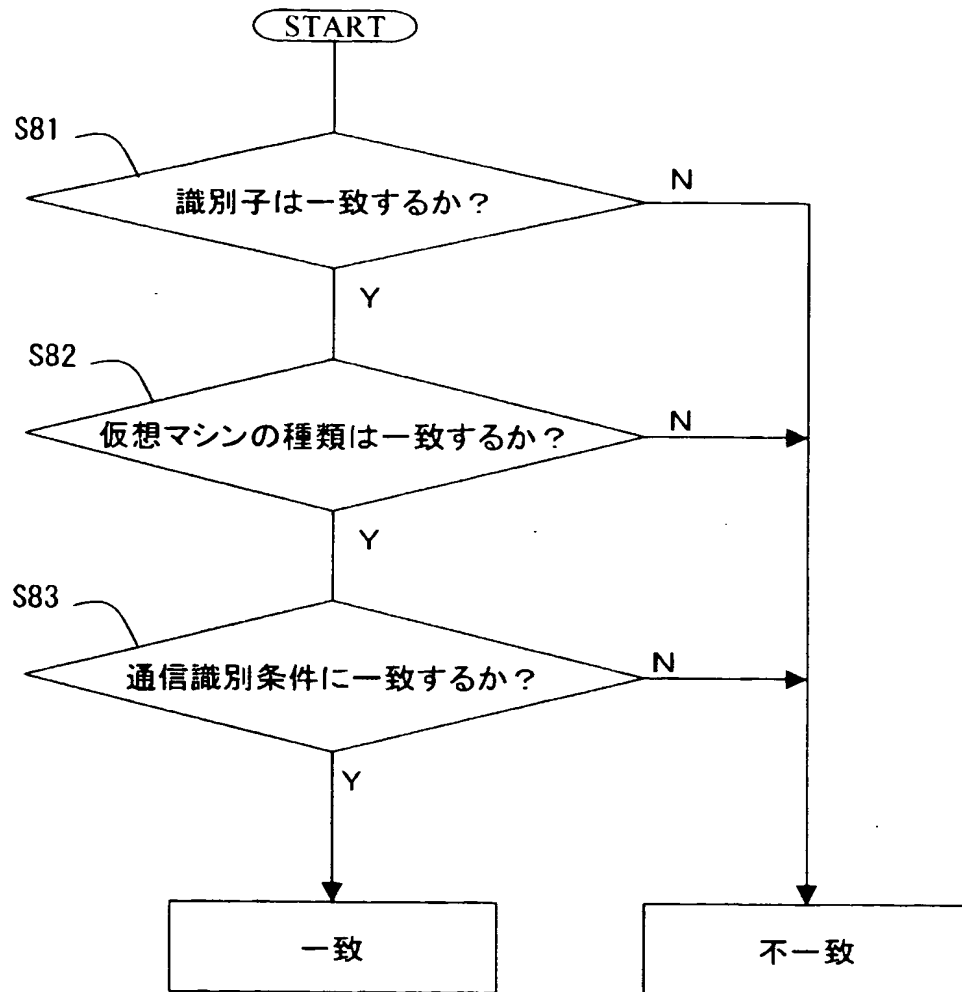
【図 6】



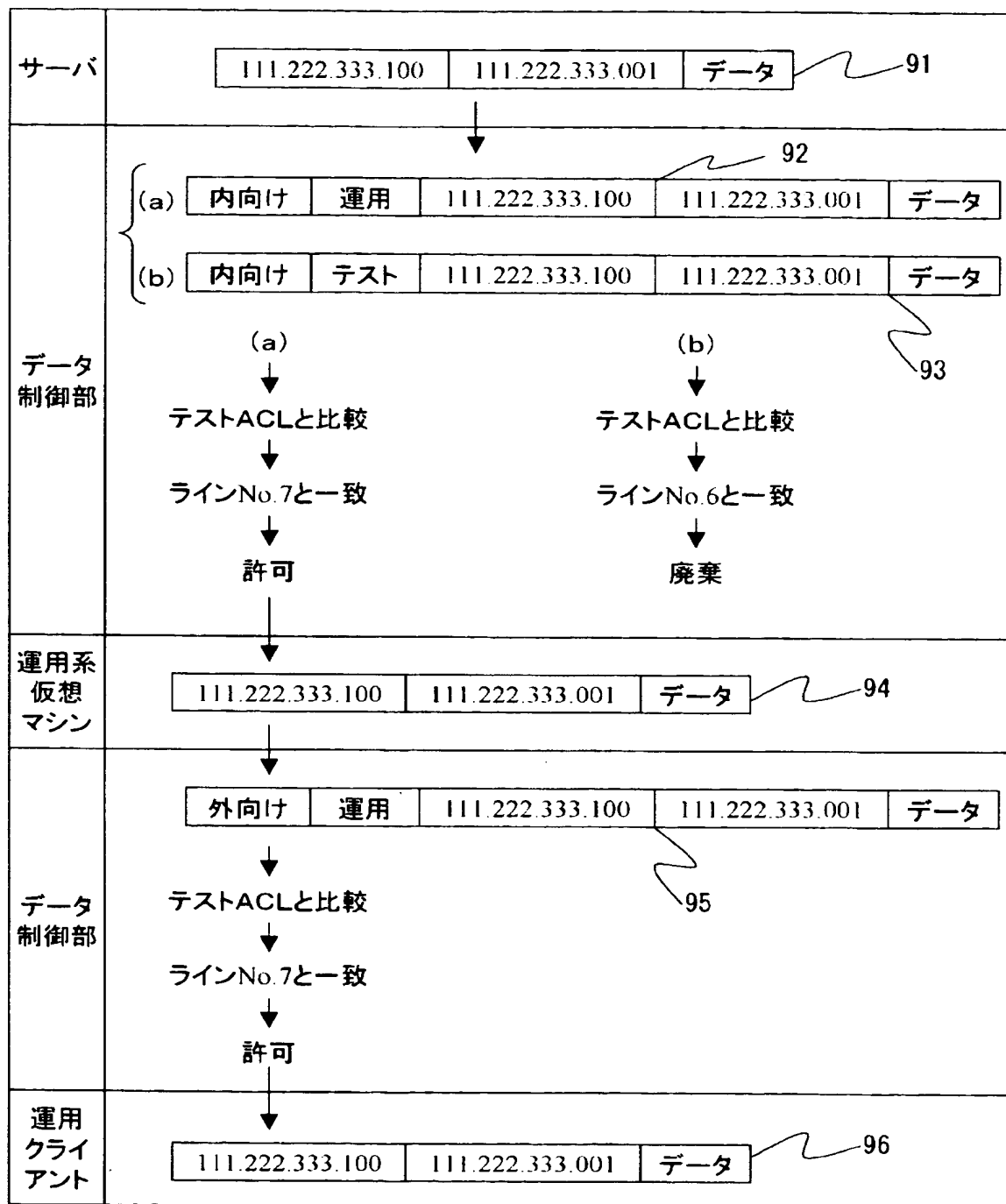
【図 7】



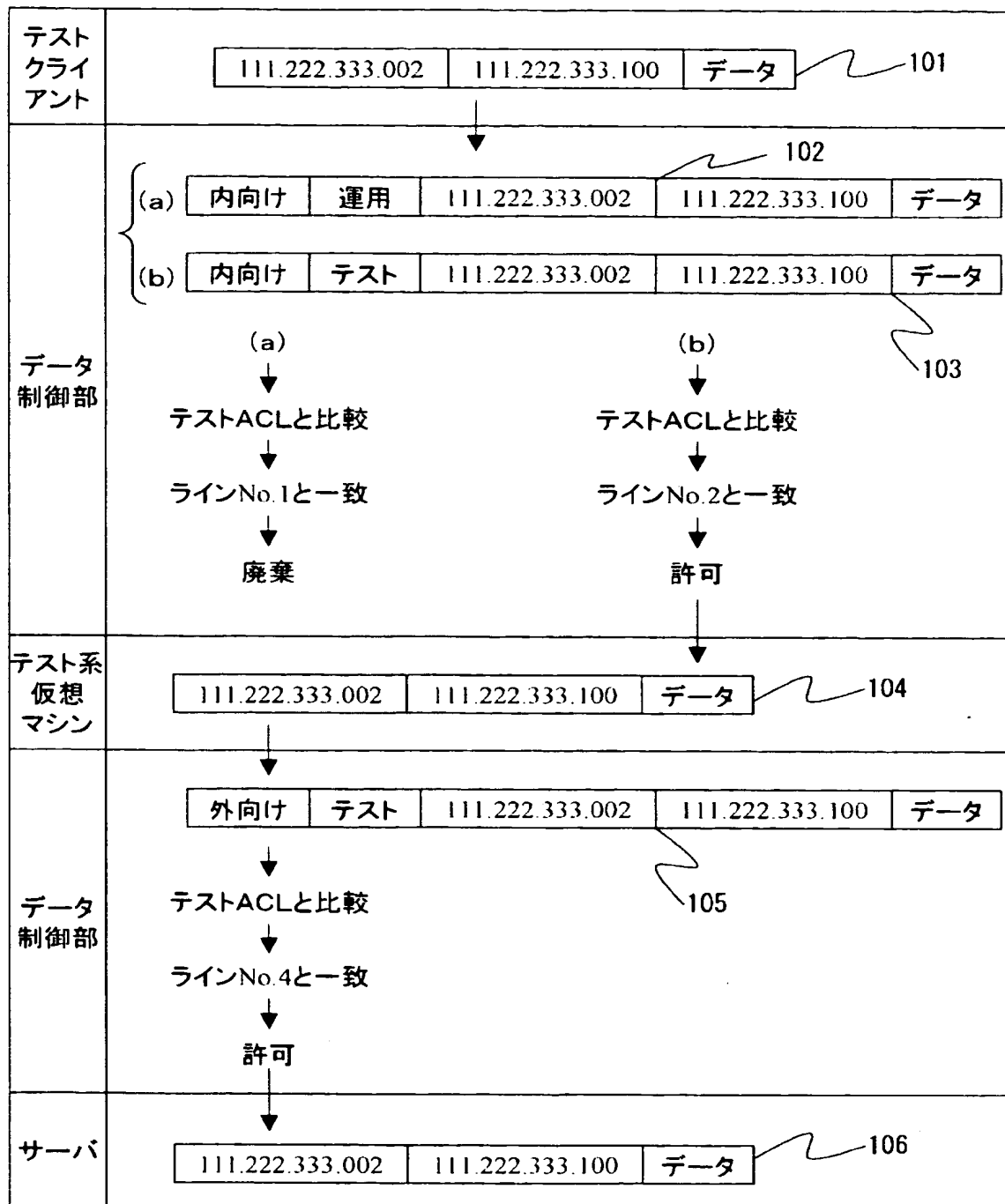
【図 8】



【図 9】



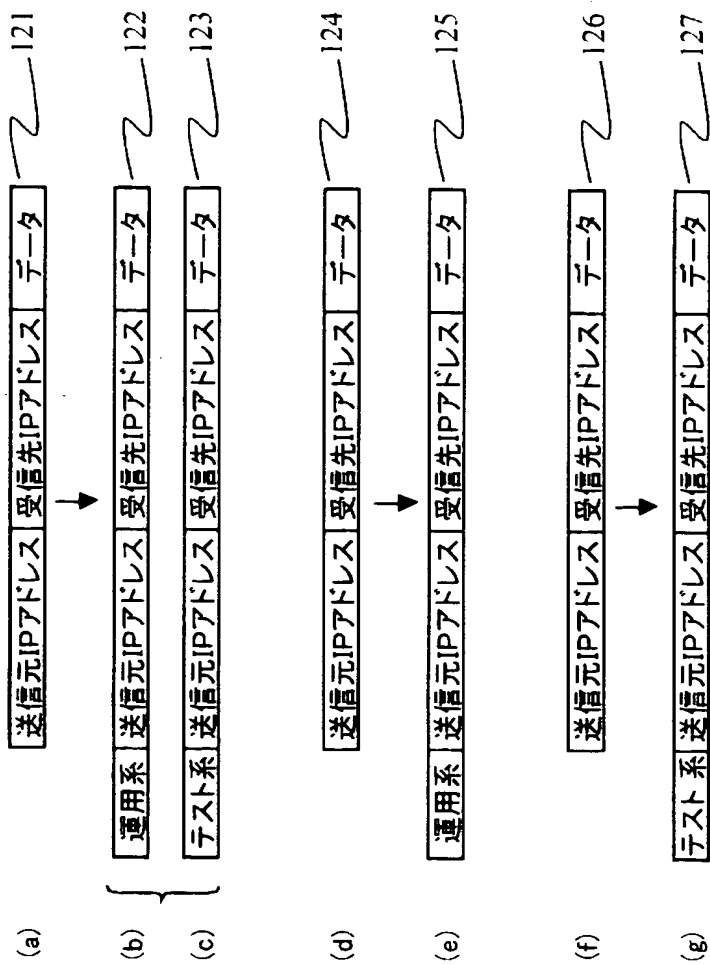
【図10】



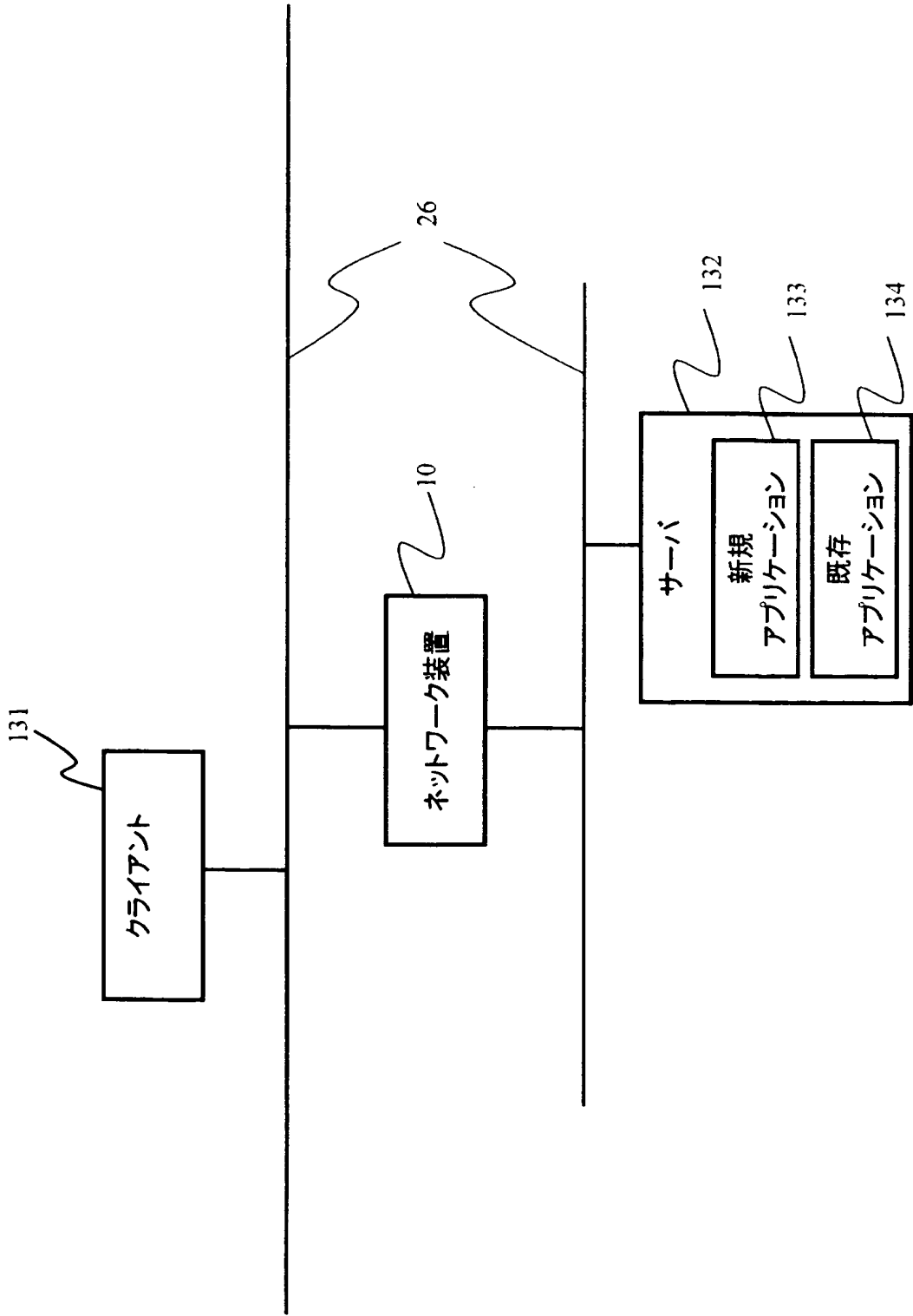
【図 11】

110				
(A) 外部機器から仮想マシン向けの通信データのテストACL				
ラインNo	仮想マシン	通信識別条件	アクション	
1	運用系	送信元又は受信先がテストクライアント	廃棄	
2	テスト系	送信元又は受信先がテストクライアント	許可	
111				
(B) 仮想マシンから外部機器向けの通信データのテストACL				
ラインNo	仮想マシン	通信識別条件	アクション	
1	運用系	送信元又は受信先がテストクライアント	廃棄	
2	テスト系	送信元又は受信先がテストクライアント	許可	
112				
(C) 両方向の通信データのテストACL ((A)、(B) に一致なかった場合)				
ラインNo	仮想マシン	通信識別条件	アクション	
1	運用系又はテスト系	受信先が本ネットワーク装置	許可	
2	テスト系	全て	廃棄	
3	運用系	全て	許可	

【図 12】



【図 13】



【図 1 4】

(A) 外部機器から仮想マシン向けの通信データのテストACL				
ラインNo.	仮想マシン	通信識別条件	アクション	
1	運用系	通信が新規アプリケーションに対するもの	廃棄	
2	テスト系	通信が新規アプリケーションに対するもの	許可	

(B) 仮想マシンから外部機器向けの通信データのテストACL				
ラインNo.	仮想マシン	通信識別条件	アクション	
1	運用系	通信が新規アプリケーションに対するもの	廃棄	
2	テスト系	通信が新規アプリケーションに対するもの	許可	

(C) 両方向の通信データのテストACL ((A)、(B) に一致しなかった場合)				
ラインNo.	仮想マシン	通信識別条件	アクション	
1	運用系又はテスト系	受信先が本ネットワーク装置	許可	
2	テスト系	全て	廃棄	
3	運用系	全て	許可	

【書類名】 要約書

【要約】

【課題】 従来、ネットワークシステムにおいて、ネットワーク装置の設定の変更やバージョンアップ及びそのテストを行う場合には、その作業を行うためにネットワークシステムの稼動を停止させる必要があった。

【解決手段】 本発明のネットワークシステムテスト方法は、ネットワークを介して接続される外部機器と該ネットワーク装置の内部の仮想マシンとの間で送受信される通信データについて、前記通信データの属性に関する条件と、前記通信データの通信を許可するか又は廃棄するかの処理内容であるアクションとが対応付けられて設定されているテストACL (Access Control List) を参照して、前記受信した通信データが、前記条件に一致するか否かを判断する判断ステップと、一致すると判断した場合には、前記通信データに対してアクションの処理内容を実施する実行ステップとを含むものである。

【選択図】 図 1

特願 2 0 0 3 - 0 9 7 4 3 1

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 2 2 3]

1. 変更年月日

1 9 9 6 年 3 月 2 6 日

[変更理由]

住所変更

住 所

神奈川県川崎市中原区上小田中 4 丁目 1 番 1 号

氏 名

富士通株式会社